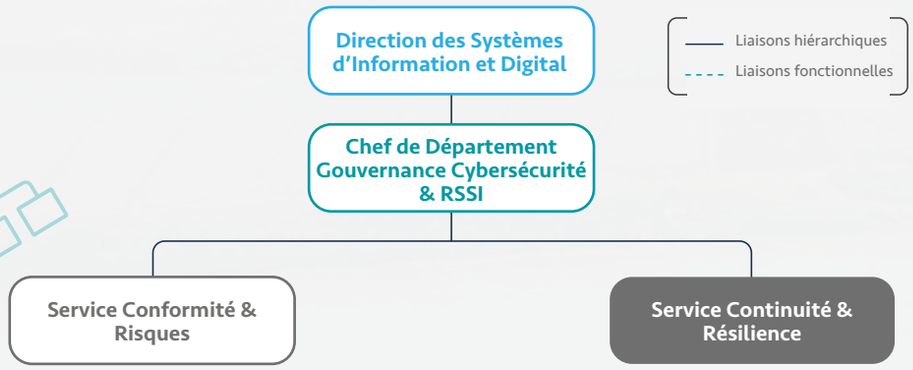
L'ONCF recrute

Chef de Service Continuité & Résilience

PROFIL POSTE

POSITION DANS L'ORGANIGRAMME



STATUT DU POSTE

Cadre supérieur

RAISON DU RECRUTEMENT

Poste vacant

LIAISONS HIÉRARCHIQUES

- **N+ 1** : Chef de Département Gouvernance Cybersécurité & RSSI
- **N- 1** : Cadres.

LIAISONS FONCTIONNELLES

- **INTERNE** : Tous les Pôles et toutes les Directions de l'ONCF ;
- **EXTERNE** : • Autorités nationales de régulation et de conformité (DGSSI, maCERT, etc.) ;
- Cabinets de conseil et d'audit spécialisés en Cybersécurité ;
- CERT / CSIRT externes ;
- Éditeurs spécialisés en solutions de Cybersécurité
- Organismes de certification.

MISSIONS PRINCIPALES DU POSTE

- Définir et mettre en œuvre la politique ainsi que les référentiels de continuité d'activité et de résilience, couvrant l'ensemble du SI ONCF (IT et OT) ;
- Mettre en place et maintenir un Système de Management de la Continuité d'Activité (SMCA) conforme à la norme ISO 22301, en assurant sa cohérence avec le SMSI et la gouvernance de Cybersécurité ;
- Élaborer et maintenir les Plans de Continuité d'Activité (PCA) et les Plans de Reprise, en cohérence avec les architectures techniques, les solutions d'hébergement et les redondances ;
- Conduire les analyses d'impact sur les activités (BIA) avec les métiers, la DSID et les équipes OT ;
- Piloter et coordonner le dispositif de gestion de crise cyber avec le SOC, le RSSI et la DSID, et assurer la coordination technique et organisationnelle au sein des comités de crise ONCF ;
- Définir et suivre les indicateurs de performance et de résilience ;
- Garantir la formation, la sensibilisation et la montée en compétence des acteurs de la continuité ;
- Assurer une veille active sur les vulnérabilités, les menaces cyber et les évolutions réglementaires (DGSSI, maCERT, éditeurs, CERT, etc.), et diffuser les alertes et recommandations aux entités concernées selon leur niveau de criticité ;
- Développer et mettre en œuvre des plans de réponse aux incidents, de remédiation et de gestion de crise, ainsi que les actions associées ;
- Piloter la réponse aux incidents de Cybersécurité, analyser leurs causes et formuler des recommandations de remédiation ;
- Collecter, analyser et contextualiser les informations de Threat Intelligence afin d'enrichir la détection, la qualification et la priorisation des alertes SOC, en assurant la continuité d'activité et la résilience Cybersécurité.

PROFIL CANDIDAT

SAVOIR-FAIRE

- Maîtrise de la norme ISO 22301 et bonnes pratiques de continuité et cyber résilience ;
- Gestion de plans de continuité d'activité (PCA) et plans de secours informatique (PSI) ;
- Analyse d'impact sur les activités (BIA) et identification des priorités de reprise ;
- Supervision des tests de continuité, bascules DC et scénarios cyber ;
- Communication et reporting clair aux parties prenantes ;
- Analyse de risques et résolution de problèmes en situation de crise ;
- Veille technologique et réglementaire sur la résilience et la Cybersécurité ;
- Capacité de prise de décision et priorisation des actions critiques ;
- Gestion de projets transverses et suivi des indicateurs de performance ;
- Maîtrise de l'analyse et de l'investigation des incidents de sécurité à partir des logs, alertes et événements collectés par le SOC ;
- Bonne maîtrise des outils technologiques du SOC et capacité à ajuster les règles de détection et les alertes ;
- Capacité à appliquer des mesures de remédiation techniques et à coordonner les actions correctives avec les équipes IT, OT et métiers ;
- Capacité à corréler et exploiter les renseignements de menace (CTI) pour renforcer l'analyse, la détection et la réponse aux incidents de sécurité ;
- Aptitude à contribuer à l'amélioration continue des use-cases, playbooks et scénarios SOC en fonction des retours d'expérience ;
- Avoir des certifications reconnues en Cybersécurité, est très souhaitable : ISO 22301, ISO 27001, CISM ou similaires.

SAVOIR-ÊTRE

- Pilotage d'équipes multidisciplinaires et coordination interservices ;
- Sens de l'engagement et de la responsabilité ;
- Esprit d'analyse, de synthèse, d'initiative et d'anticipation ;
- Excellente communication de crise en cas de cyberattaques majeures ;
- Rigueur, sens de la méthode et probité ;
- Développement des compétences du service et orientation vers l'atteinte des objectifs ;

EXPÉRIENCE PROFESSIONNELLE

Une expérience minimale de 5 ans en Cybersécurité, incluant des activités de continuité d'activité et cyber-résilience.

FORMATION

Diplôme d'Ingénieur ou Master, lauréat d'une grande école d'ingénieurs, d'une université ou équivalent, en cybersécurité ou dans un domaine équivalent.

CONDITIONS D'EMPLOI

TYPE DE CONTRAT : CDI | **LIEU DE TRAVAIL : RABAT** | **DÉPLACEMENT À PRÉVOIR : OUI**

PROCÉDURE DE SÉLECTION

Seuls les diplômes délivrés par les établissements publics ou ceux disposant d'une attestation d'équivalence délivrée par les autorités compétentes seront éligibles.

Le dossier de candidature doit comprendre les documents suivants :

- Diplôme ;
- Carte nationale d'identité électronique ;
- CV actualisé ;
- Attestation(s) / Certificat(s) de travail couvrant l'ensemble des années d'expérience exigées.

Tout dossier incomplet ou ne correspondant pas au profil recherché sera automatiquement écarté.

Veuillez renseigner et transmettre la demande de candidature en utilisant le lien ci-dessous :

https://oncf.etalent.ma/

Seules les candidatures reçues via ce lien seront traitées.

Les candidats intéressés par cette offre doivent soumettre leur candidature au plus tard le 22 Juin 2026 à 23h00.

SCANNER LE CODE QR

GET STARTED